IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

THOMAS JONES and LEAH SIMIONE, *on behalf of themselves and all others similarly situated*, Plaintiffs, vs. ONIX GROUP, LLC, Defendant	Case No: **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Thomas Jones and Leah Simione ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this class action lawsuit against Defendant Onix Group LLC, ("Defendant" or "Onix"). Plaintiffs seek to obtain damages, restitution, and injunctive relief for themselves and the Class, as defined below. Plaintiffs set forth the following allegations upon information and good faith belief, except as to their own actions, the investigation of their counsel, and certain facts that are a matter of public record.

INTRODUCTION

1. This class action lawsuit seeks to address Onix's abject failure to provide necessary data security measures to prevent the recent targeted cyberattack and data breach of its network that resulted in the unauthorized access of highly sensitive patient data. Plaintiffs bring this class action against Onix for its failure to secure and safeguard approximately 319,500 individuals' personally identifiable information ("PII") and personal health information ("PHI") (collectively, "Private Information").

2. Onix is a business conglomerate based in Kennett Square, Pennsylvania that operates in the hospitality, commercial real estate and healthcare industries.[1]

3. According to Onix's notice, Defendant "experienced a ransomware incident" on March 27, 2023, affecting its internal computer systems between the period of March 20 and March 27, 2023, which resulted in unauthorized access to Private Information (the "Data Breach").[2]

4. The Data Breach impacted Onix's following groups: Addiction Recovery Systems, Cadia Healthcare, Physician's Mobile X-Ray, Onix Group, and Onix Hospitality Group.[3]

5. As a condition of receiving medical services and rehabilitation treatment, Onix's patients are required to provide Onix with their sensitive and private information, including PII and PHI.

6. As revealed thus far, the following types of information were compromised in the Data Breach: names, Social Security numbers, birthdates, scheduling, billing, and unspecified "clinical information" regarding care at one of Onix's affiliated entities. The compromised files also contained information maintained for human resources purposes, including names, Social Security numbers, direct deposit information, and health plan enrollment information.[3]

7. While Onix has stated that the Data Breach was the result of a "ransomware incident" undertaken by an unauthorized third party, it failed to disclose the identity of the unauthorized third party and has not publicly disclosed whether or not a ransomware demand was made and/or paid. In fact, Onix did not offer any assurances or evidence that all impacted Private Information or copies thereof have been recovered or destroyed.

---

[1] https://www.onixgroup.com/about-onix/ (last visited July 6, 2023).

[2] *Notice of Data Security Incident*, available at https://www.onixgroup.com/wp-content/uploads/2023/05/Onix-Notice-of-Data-Security-Incident.pdf (last accessed July 6, 2023).

[3] *Id.*

8. Onix also failed to explain why it waited more than two months after first becoming aware of the incident to provide notice of the Data Breach.

9. Acknowledging the patent insufficiency of its data security practices, Onix now states that it has since "strengthened the security of its systems."

10. Sadly, Onix's self-serving representations that it is now taking its data security obligations seriously—despite the incredible number of similar data security incidents in the healthcare industry in recent months and years—the Data Breach was a direct result of Onix's failure to implement cybersecurity procedures and protocols necessary to protect individuals' PII and PHI from the foreseeable threat of a cyberattack.

11. By taking possession and control of Plaintiffs' and Class Members' Private Information for its own pecuniary benefit, Onix assumed a duty to implement and to maintain reasonable and adequate security measures to secure, protect and safeguard this Private Information against unauthorized access and disclosure. Onix also had a duty to adequately safeguard this Private Information further to industry standards and duties imposed by statutes, including HIPAA regulations and Section 5 of the Federal Trade Commission Act (the "FTCA").

12. Onix breached these duties by, among other things, failing to implement and to maintain reasonable security procedures and practices to protect patients' and other individuals' Private Information from unauthorized access and disclosure.

13. The exposure of a person's PII and PHI through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. As a result of the Data Breach, Plaintiffs and Class Members are at imminent and substantial risk of experiencing various types of misuse of their Private Information in the coming years, including but not limited to,

unauthorized access to email accounts, tax fraud, and identity theft—including medical identity theft.

14. Mitigating that risk, to the extent it is even possible to do so, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and take several additional prophylactic measures.

15. Plaintiffs bring this action on behalf of themself and individuals in the United States whose Private Information was exposed as a result of the Data Breach. They seek to hold Onix responsible for the harms resulting from the massive and preventable disclosure of such sensitive and personal information.

16. Plaintiffs seek remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and declaratory and injunctive relief including improvements to Onix's data security systems, future annual audits, and adequate credit monitoring services funded by Onix.

JURISDICTION & VENUE

17. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5 million, and many members of the class are citizens of states different from Defendant.

18. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

19. The Court has general personal jurisdiction over Defendant because Onix resides in, has its principal place of business, and does business in the Commonwealth of Pennsylvania.

20. Additionally, the Court has specific personal jurisdiction over Defendant because a substantial part of the events giving rise to the claims occurred in Pennsylvania.

21. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

THE PARTIES

Plaintiffs

22. Plaintiff Thomas Jones is a resident of New Jersey. He provided his PII and PHI to Addiction Recovery Services, one of Onix's affiliated groups, and was notified via letter dated May 26, 2023, that his information was compromised in the Data Breach.

23. Upon receipt of Plaintiff Jones' Private Information, Addiction Recovery Services entered it into Onix's database wherein his PII and PHI was stored and maintained. In maintaining his Private Information, Onix expressly and impliedly promised to safeguard Plaintiff Jones' PII and PHI. However, Onix did not take proper care of this sensitive data, leading to its exposure as a direct result of its inadequate security measures.

24. Plaintiff Leah Simione is a resident of New Jersey. She provided her PII and PHI to Addiction Recovery Services, one of Onix's affiliated groups, and was notified via letter dated May 26, 2023, that her information was compromised in the Data Breach.

25. Upon receipt of Plaintiff Simione's information, Addiction Recovery Services entered it into Onix's database wherein the PII and PHI was stored and maintained. In maintaining her information, Onix expressly and impliedly promised to safeguard Plaintiff Simione's PII and PHI. However, Onix did not take proper care of this sensitive data, leading to its exposure as a direct result of its inadequate security measures.

26. In the months and years following the Data Breach, Plaintiffs and other Class Members will experience a slew of harms because of Onix's ineffective data security measures.

Some of these harms will include fraudulent charges, medical procedures ordered in patient's names without their permission, and potentially more.

Defendant

27. Defendant Onix Group LLC is a 501(c) Pennsylvania-based business administrator with its principal place of business located at 150 Onix Drive in Kennett Square, Pennsylvania 19348.

FACTUAL ALLEGATIONS

A. Onix Group's Business

28. The Onix Group was established in 1987 "for the purpose of owning, developing and operating various real estate investments principally for its own account – while also providing management and consulting services to others."[4] It operates eight hotels (with three more under development) and claims to manage "a diverse collection of commercial real estate, including commercial shopping centers, office buildings, retail pad sites and residential properties."[5]

29. The Onix Group also has a healthcare division which operates addiction recovery clinics, skilled nursing facilities, a pharmacy and a physician group in the Mid-Atlantic region.[6]

30. As a condition of providing services to the company's healthcare division, Onix requires that its customers entrust it with their PII and PHI.

31. Because of the highly sensitive and personal nature of the information Onix acquires and stores with respect to patients and other individuals, Onix, upon information and belief, promises to, among other things: keep customers' PHI private; comply with healthcare

---

4 https://www.onixgroup.com/about-onix/.

5 *Id*.

6 https://www.onixgroup.com/businesses/ (last visited July 6, 2023).

industry standards related to data security and Private Information; inform customers and patients of legal duties and comply with all federal and state laws protecting customers' and patients' Private Information; only use and release customers' Private Information for reasons that relate to medical care and treatment; and provide adequate notice to customers if their Private Information is disclosed without authorization.

32. As a HIPAA covered entity, Onix is required to implement adequate safeguards to prevent unauthorized use or disclosure of Personal Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured protected health information as in the case of this Data Breach.

33. However, Onix did not maintain adequate security to protect its systems from infiltration by cybercriminals, and it waited nearly two months to disclose the Data Breach publicly.

34. Plaintiffs and Class Members include patients or clients of Onix, and individuals with a potential or actual employment relationship, who entrusted Onix with their Private Information.

B. Onix is a HIPAA Covered Entity

35. The healthcare division of Onix is a HIPAA covered entity that provides healthcare services. As a regular and necessary part of its business, Onix collects and custodies the highly sensitive PII of its clients' patients and health plan Members. Onix is required under federal and state law to maintain the strictest confidentiality of the patient's Private Information that it requires, receives, and collects, and Onix is further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

36. As a HIPAA covered entity, Onix is required to ensure that it will implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

37. Due to the nature of Onix's business, which includes providing a range of medical and rehabilitation services, Onix would be unable to engage in its regular business activities without collecting and aggregating Private Information that it knows and understands to be sensitive and confidential.

38. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Onix assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

39. Plaintiffs and Class Members are or were patients who received health-related or medical services from Onix and directly or indirectly entrusted Onix with their Private Information.

40. Plaintiffs and the Class Members relied on Onix to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of the Private Information. Plaintiffs and Class Members reasonably expected that Onix would safeguard their highly sensitive information and keep their Private Information confidential.

41. As described throughout this Complaint, Onix did not reasonably protect, secure, or store Plaintiffs' and the Class Members' sensitive Private Information prior to, during, or after the Data Breach.

42. Instead, Defendant enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information Onix maintained. Consequently, cybercriminals circumvented Onix's security measures, resulting in a significant data breach.

C. The Data Breach & Notice Letter

43. According to the notice Onix provided to Plaintiffs and Class Members, Onix was subject to a cybersecurity attack between March 20-27, 2023, which culminated in ransomware of its patients' and/or clients' PHI or PII on March 27, 2023.

44. Onix's Notice of the Data Security Incident vaguely states that in response, Defendant "took immediate action to secure systems and launched an investigation with help from cybersecurity experts."

45. As a HIPAA associated business entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk of which Onix was aware and knew it had a duty to guard against.

46. This is particularly true because the targeted attack was a ransomware attack. It is well-known that healthcare businesses such as Onix, which collect and store the confidential and sensitive PII/PHI of hundreds of thousands of individuals, are frequently targeted by ransomware attacks.

47. Further, ransomware attacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

48. In fact, the vast majority of ransomware incidents are caused by a combination of poor user practices, lack of cybersecurity training, and weak passwords or access management.[7]

49. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients, like Plaintiffs and Class Members.

50. Despite learning that the Data Breach compromised PII and PHI on March 27, 2023, Onix inexplicably waited over two months following the completion of its investigation to notify the impacted individuals of the Data Breach and the need for them to protect themselves against fraud and identity theft.

51. Due to Onix's inadequate security measures and its delayed notice to victims, Plaintiffs and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

52. Onix had obligations created by HIPAA, contract, industry standards, common law, and its own promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

53. Plaintiffs and Class Members provided their Private Information to Onix, or its affiliates, with the reasonable expectation and mutual understanding that Onix would comply with its obligations to keep such information confidential and secure from unauthorized access.

54. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Onix assumed legal and equitable duties and knew, or should have

[7] *Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs worldwide as of 2020* (May 3, 2023), available at https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/ (last visited July 6, 2023).

known, that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

55. Onix's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

56. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their personal information. Plaintiffs and Class Members would not have allowed Onix or anyone in Onix's position to receive their Private Information had they known that Onix would fail to implement industry standard protections for that sensitive information.

57. As a result of Onix's negligent and wrongful conduct, Plaintiffs' and Class Members' highly confidential and sensitive Private Information was left exposed to cybercriminals.

D. Onix Failed to Comply with FTC Guidelines

58. Onix was prohibited by the FTCA from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTCA. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

59. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

60. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses.

61. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[8]

62. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[9]

63. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

64. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

65. These FTC enforcement actions include actions against healthcare providers and partners like Onix. *See, e.g., In the Matter of LabMD, Inc., A Corp.*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that

---

[8] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), available at https://www.bulkorder.ftc.gov/publications/protecting-personal-information-guide-business (last visited July 6, 2023).

[9] *Id*.

LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTCA.")

66. Onix failed to properly implement basic data security practices.

67. Onix's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

68. Onix was at all times fully aware of the obligation to protect the Private Information of customers and patients. Onix was also aware of the significant repercussions that would result from its failure to do so.

E. Onix Failed to Comply with Industry Standards

69. As shown above, experts studying cybersecurity routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

70. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Onix, including but not limited to educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

71. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

72. Onix failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

73. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Onix failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

F. Onix Violated its HIPAA Obligations to Safeguard the Private Information

71. Onix is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

72. Onix is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[10] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

73. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information that is kept or transferred in electronic form.

[10] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

74. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

75. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

76. HIPAA's Security Rule requires Onix to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

71. HIPAA also requires Onix to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Onix is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

72. HIPAA and HITECH also obligated Onix to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

73. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Onix to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[11]

74. HIPAA further requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

75. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

76. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318.

77. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[12] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says,

---

[11] *See* Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

[12] *See* http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited July 6, 2023).

"represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[13]

74. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Onix left unguarded.

75. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

76. A Data Breach such as the one Onix experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40

77. The Data Breach resulted from a combination of insufficiencies that demonstrate Onix failed to comply with safeguards mandated by HIPAA regulations.

G. Onix Breached its Duty to Safeguard Plaintiffs' & Class Members' Private Information

78. In addition to its obligations under federal and state laws, Onix owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Onix owed a duty to

[13] *See id.*

Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

79. Onix owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

80. Onix owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

81. Onix owes a legal duty to secure consumers' PII and PHI and to timely notify consumers of a data breach.

82. Onix breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Onix's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to detect unauthorized ingress into its systems;

f. Failing to implement and monitor reasonable network segmentation to detect unauthorized travel within its systems, including to and from areas containing the most sensitive data;

g. Failing to detect unauthorized exfiltration of the most sensitive data on its systems;

h. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

i. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

j. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

k. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

l. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

m. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

n. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

o. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

p. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

q. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

r. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTCA;

s. Failing to adhere to industry standards for cybersecurity as discussed above; and

t. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

83. Onix negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

84. Had Onix remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Onix could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential PII.

85. However, due to Onix's failures, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Onix.

H. Onix Knew or Should Have Known that Criminals Target Private Information

78. Onix's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the breach.

79. At all relevant times, Onix knew, or should have known, its patients', Plaintiffs', and all other Class Members' Private Information was a target for malicious actors.

80. Despite such knowledge, Onix failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' Private Information from cyber- attacks that Onix should have anticipated and guarded against.

81. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients and/or plan Members, like Plaintiffs and Class Members.

82. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[14]

83. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[15]

84. Further, a 2022 report released by IBM Security states that for 12 consecutive years the healthcare industry has had the highest average cost of a data breach and as of 2022 healthcare data breach costs have hit a new record high.[16]

85. Private Information is a valuable property right and its value as a commodity is measurable.[17] "Firms are now able to attain significant market valuations by employing business

---

[14] *2022 Breach Barometer*, PROTENUS, available at https://blog.protenus.com/key-takeaways-from-the- 2022-breach-barometer (last visited July 6, 2023).

[15] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), available at: https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited July 6, 2023).

[16] *Cost of a Data Breach Report* 2022, IBM Security, available at https://www.ibm.com/downloads/cas/3R8N1DZJ (last visited July 6, 2023).

[17] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of

models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[18]

86. American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[19]

87. Private Information is so valuable to identity thieves that once Private Information has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

88. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, Private Information, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

89. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[20] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10

[personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible[.]"); Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192 (last visited July 6, 2023).

[18] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en (last visited July 6, 2023).

[19] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (last visited July 6, 2023).

[20] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.") (last visited July 6, 2023).

personal identifying characteristics of an individual." A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[21]

90. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[22] According to a report released by the FBI Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[23]

91. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[24]

---

[21] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), available at https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited July 6, 2023).

[22] Adam Greenberg, *Health insurance credentials fetch high prices in the online black market*, SC MAGAZINE (July 16, 2013), available at https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market (last visited July 6, 2023).

[23] *See Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIVISION (Apr. 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf (last visited July 6, 2023).

[24] *Editorial: Why do criminals target medical records*, The HIPAA Journal (Oct. 14, 2022), available at https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last visited July 6, 2023).

92. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health, insurance information, and medical and clinical data, and that information can be easily monetized."[25]

93. The HIPAA Journal article goes on to explain that patient records, like those stolen from Onix, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."

94. Criminals can use stolen Private Information to extort a financial payment by "leveraging details specific to a disease or terminal illness."[26] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion…By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[27]

95. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies

---

25 *Id.*

26 *What Happens to Stolen Healthcare Data* (Oct. 30, 2019), available at https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon

27 *Id.*

confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[28]

96. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

97. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[29]

98. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, entities like and hospitals are attractive to ransomware criminals because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[30]

---

[28] Janice Y. Tsai, *et al*., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), available at https://www.guanotronic.com/~serge/papers/weis07.pdf .

[29] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited July 6, 2023).

[30] *Ransomware Attacks on Hospitals Put Patients at Risk* (May 18, 2022), available at https://stateline.org/2022/05/18/ransomware-attacks-on-hospitals-put-patients-at-risk/ (last visited July 6, 2023).

99. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[31]

100. Onix was on notice that the FBI has recently been concerned about data security in the healthcare industry.

101. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them.

102. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[32]

103. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[33]

104. As implied by the above AMA quote, stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiffs and Class Members.

---

[31] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack, Security Magazine* (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited July 6, 2023).

[32] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited July 6, 2023).

[33] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited July 7, 2023).

105. Onix was on notice that the federal government has been concerned about healthcare company data encryption practices. Onix knew its employees accessed and utilized protected health information in the regular course of their duties, yet it appears that information was not encrypted.

106. The OCR urges the use of encryption of data containing sensitive personal information. As far back as 2014, HHS fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, formerly OCR's deputy director of health information

privacy, stated in 2014 that "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[34]

107. As a HIPAA covered business associate, Onix should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Private Information stored in its unprotected files.

I. Cyberattacks & Data Breaches Cause Disruption & Put Consumers at an Increased Risk of Fraud & Identity Theft.

108. Cyberattacks and data breaches at healthcare companies like Onix are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

109. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[35]

---

[34] "Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html (last visited July 6, 2023).

[35] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*,

110. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[36]

111. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[37]

112. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names.

113. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired

---

PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last visited July 6, 2023).

[36] *See* Sung J. Choi, *et al*., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019), available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last visited July 6, 2023).

[37] *See* U.S. Gov. Accounting Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007), available at https://www.gao.gov/assets/gao-07-737.pdf (last visited July 6, 2023).

information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

114. Theft of Private Information is serious. The FTC warns consumers that identity thieves use Private Information to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.

115. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[38]

116. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

117. Identity thieves can also use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition,

[38] *See* Federal Trade Commission, https://www.identitytheft.gov/#/Steps (last visited July 6, 2023).

identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

118. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[39]

119. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[40]

120. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Private Information on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

121. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the Private Information stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful

---

[39] *See, e.g.,* John T. Soma, *et al.*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[40] *See* Federal Trade Commission, *Medical Identity Theft*, https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited July 6, 2023).

forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

122. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

123. Recent reports confirm that large batches of data—and perhaps the entire batch of stolen data—is already available for sale on the dark web and in hacking forums, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

124. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.

125. Cyber criminals may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[41]

126. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number:** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refund, employment—even using your identity in bankruptcy and other legal matters. It's hard to change your Social

[41] *See* https://www.gao.gov/assets/gao-07-737.pdf

> Security number and it's not a good idea because it is connected to your lift in so many ways.[42]

127. For instance, with a stolen Social Security number, which is only one subset of the Private Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.

128. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

129. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[43]

---

[42] *Dark web Monitoring: What You Should* Know (mar. 19, 2019), available at https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/; *see, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, available at https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited July 6, 2023).

[43] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited July 6, 2023).

130. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like Onix is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

131. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[44] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web." [45]

132. The medical information, PHI, which was exposed is also highly valuable. PHI can sell for as much as $363 according to the Infosec Institute.[46]

133. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to PII, they *will use it*.[47]

134. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[48]

---

[44] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web* (Nov. 15, 2017), available at https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web (last visited July 6, 2023).

[45] *Dark Web Monitoring: What You Should Know*, *supra* note 42.

[46] Center for Internet Security, *Data Breaches: In the Healthcare Sector*, available at https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited July 6, 2023).

[47] *Id.*

[48] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families,*

135. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the victim has suffered the harm.

136. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[49]

137. Theft of PII is even more serious when it includes theft of PHI. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

138. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. According to Kaiser Health News, "medical-related identity theft accounted for 43

Friends, and Workplaces, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/publication/identity-theft-the-aftermath-study/ (last visited July 6, 2023).

[49] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/ (last visited July 6, 2023).

percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[50] "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. *Id.* "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities." *Id.*

139. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[51] It "is also more difficult to detect, taking almost twice as long as normal identity theft." In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use Private Information "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[52] The FTC also warns, "If the thief's health information is mixed with yours, it could affect the medical care you're able to get or the health insurance benefits you're able to use. It could also hurt your credit."[53]

140. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

---

50 Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited July 6, 2023).

51 Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIVACY FORUM 6 (Dec. 12, 2017), https://www.worldprivacyforum.org/2017/12/new-report-the-geography-of-medical-identity-theft/ (last visited July 6, 2023).

52 *See* https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft.

53 *See id*.

- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.

141. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

142. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[54]

---

[54] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), https://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf (last visited July 6, 2023).

143. Cybercriminals can post stolen Private Information on the cyber black-market for years following a data breach, thereby making such information publicly available.

144. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened. [55] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[56]

145. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[57]

146. It is within this context that Plaintiffs and all other Class Members must now live with the knowledge that their Private Information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

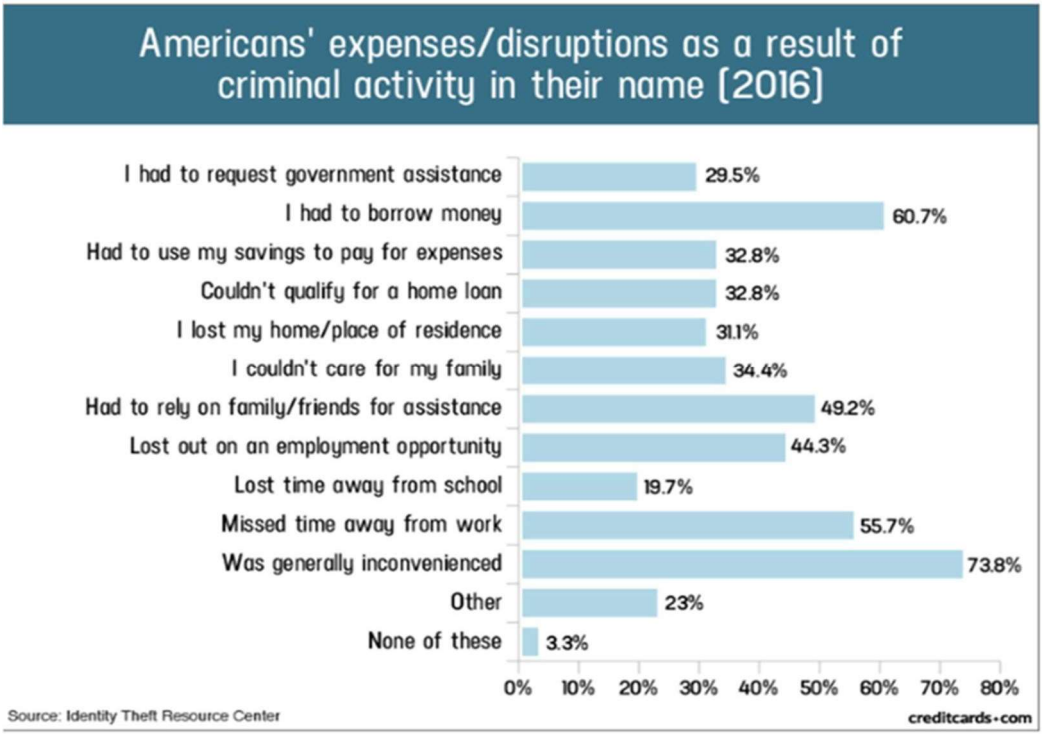
147. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information.

---

[55] *See Medical ID Theft Checklist*, available at https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited July 6, 2023).

[56] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages")*, available at https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited July 6, 2023).

[57] U.S. DOJ, Office for Victims of Crime, *Expanding Services to Reach Victims of Identity Theft and Financial Fraud*, available at https://ovc.ojp.gov/sites/g/files/xyckuh226/files/pubs/ID_theft/pfv.html (last visited July 6, 2023).



148. Victims of the Data Breach, like Plaintiffs and Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach. *Id.*

149. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have had their Private Information exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and Class Members must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

150. Plaintiffs and Class Members have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;

b. Trespass, damage to, and theft of their personal property, including Private Information;

c. Improper disclosure of their Private Information;

d. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their Private Information being in the hands of criminals and having already been misused;

e. The imminent and certainly impending risk of having their confidential medical information used against them by spam callers to defraud them;

f. Damages flowing from Onix's untimely (and in some cases, non-existent) and inadequate notification of the Data Breach;

g. Loss of privacy suffered as a result of the Data Breach;

h. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

i. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

j. The loss of use of and access to their credit, accounts, and/or funds;

k. Damage to their credit due to fraudulent use of their Private Information; and

l. Increased cost of borrowing, insurance, deposits, and other items which are adversely affected by a reduced credit score.

151. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Onix, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Onix has shown itself to be wholly incapable of protecting Plaintiffs' and Class Members' Private Information.

152. Plaintiffs and Class Members also have an interest in ensuring that their personal information that was provided to Onix is removed from Onix's unencrypted files.

153. Onix itself acknowledged the harm caused by the Data Breach because it offered Plaintiffs and Class Members the inadequate 12 months of identity theft protection and credit monitoring services. This limited identity theft monitoring is, however, inadequate to protect Plaintiffs and Class Members from a lifetime of identity theft risk.

154. At Onix's suggestion, Plaintiffs are trying to mitigate the damage that Onix has caused them. Given the kind of Private Information Onix made accessible to hackers, however, Plaintiffs are certain to incur additional damages. Because identity thieves have their Private Information, Plaintiffs and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[58]

155. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. For this reason, Onix knew or should have known about these dangers and strengthened its data security accordingly. Onix was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

J. The Data Breach Was Foreseeable and Preventable

156. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some

---

[58] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html (last visited July 6, 2023).

of the biggest cybersecurity breaches.[59]

157. Companies providing services to the healthcare industry, such as Onix, have been prime targets for cyberattacks. As early as August 2014, the FBI specifically warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[60]

158. Onix should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the Private Information that it collected and maintained.

159. Onix was clearly aware of the risks it was taking and the harm that could result from inadequate data security, and it could have prevented this Data Breach.

160. Data disclosures and data breaches are preventable. As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[61] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised[.]"[62]

---

59 *See, e.g.*, CSO Online, *The 15 biggest data breaches of the 21st century*, available at https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html (last visited July 6, 2023).

60 https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idINKBN0GK24U20140820 (last visited July 6, 2023).

61 Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

62 *Id.*

161. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[63]

162. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[64]

163. The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems.

164. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

165. Upon information and belief, Onix failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, Onix also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the

---

63 *Id.*

64 FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 6, 2023).

Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

166. In August 2022, the Consumer Finance Protection Bureau (CFPB) published a circular on data security. The CFPB noted that "[w]idespread data breaches and cyberattacks have resulted in significant harms to consumers, including monetary loss, identity theft, significant time and money spent dealing with the impacts of the breach, and other forms of financial distress," and the circular concluded that the provision of insufficient security for consumers' data can violate the prohibition on "unfair acts or practices" in the Consumer Finance Protection Act (CFPA).[65]

167. Given that Onix was storing the Private Information of more than 5,000,000 individuals, Onix could and should have implemented all of the above measures to prevent and detect ransomware attacks. These are basic, common-sense email security measures that every business, not only healthcare businesses, should be doing. Onix, with its heightened standard of care should be doing even more.

168. Specifically, among other failures, Onix had far too much confidential unencrypted information held on its systems. Such Private Information should have been segregated into an encrypted system.[66]

169. Indeed, the United States Department of Health and Human Services' Office for Civil Rights urges the use of encryption of data containing sensitive personal information, stating "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[67]

---

[65] Consumer Financial Protection Circular, 2022-4, available at https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/ (last visited July 6, 2023).

[66] *See, e.g.*, Adnan Raja, *How to Safeguard Your Business Data with Encryption*, Aug. 14, 2018, https://www.digitalguardian.com/blog/how-safeguard-your-business-data-encryption (last visited July 6, 2023).

170. Charged with handling sensitive Private Information, including healthcare information, Defendant knew, or should have known, the importance of safeguarding its patients' Private Information that was entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on its patients after a breach. Onix failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

171. With respect to training, Defendant specifically failed to:

- Implement a variety of anti-ransomware training tools, in combination, such as computer-based training, classroom training, monthly newsletters, posters, login alerts, email alerts, and team-based discussions;
- Perform regular training at defined intervals such as bi-annual training and/or monthly security updates; and
- Craft and tailor different approaches to different employees based on their base knowledge about technology and cybersecurity.

172. The Private Information was also maintained on Onix's computer system in a condition vulnerable to cyberattacks, such as through the infiltration of Defendant's systems through ransomware attacks. The mechanism of the cyberattack and the potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Onix, and thus Onix was on notice that failing to take reasonable steps necessary to secure the Private Information from those risks left it in a vulnerable position.

173. In sum, this Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all confidential information.

174. Plaintiffs and Class Members entrusted their Private Information to Onix as a condition of receiving healthcare related services. Plaintiffs and Class Members understood and expected that Onix or anyone in Onix's position would safeguard their Private Information against

[67] "Stolen Laptops Lead to Important HIPAA Settlements," *supra* note 34.

cyberattacks, delete or destroy Private Information that Onix was no longer required to maintain, and timely and accurately notify them if their Private Information was compromised.

K. The Monetary Value of Privacy Protections & Private Information

175. The fact that Plaintiffs' and Class Members' Private Information was stolen means that Class Members' information is likely for sale by cybercriminals and will be misused in additional instances in the future. Indeed, there is already evidence that Plaintiffs' Private Information is on the dark web.

176. At all relevant times, Defendant was well aware that the Private Information it collects from Plaintiffs and Class Members is highly sensitive and of significant value to those who would use it for wrongful purposes.

177. As discussed above, Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[68]

178. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[69]

[68] *See* Federal Trade Commission, *What to Know About Identity Theft*, https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited July 6, 2023).

[69] *See Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.govinfo.gov/app/details/FR-2001-02-07/01-3194 (last visited July 6, 2023).

179. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[70]

180. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[71]

181. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information. The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

182. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their

---

[70] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), https://www.wsj.com/articles/SB10001424052748703529004576160764037920274 (last visited July 6, 2023).

[71] *See Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited July 7, 2023).

data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[72]

183. As discussed above, the value of Plaintiffs' and Class Members' Private Information on the black market is substantial.

184. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment.

185. The ramifications of Onix's failure to keep its patients' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

186. Victims may not realize their identity has been compromised until long after it has happened.[73] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[74]

187. As discussed herein, breaches are particularly serious in healthcare industries, with healthcare related data among the most private and personally consequential, as set forth above.

---

[72] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), available at https://bjs.ojp.gov/library/publications/victims-identity-theft-2018 (last visited July 7, 2023).

[73] *See Survey on Medical Identity Theft*, Ponemon Institute (June 2012), available at https://www.ponemon.org/local/upload/file/Third_Annual_Survey_on_Medical_Identity_Theft_FINAL.pdf (last visited July 7, 2023).

[74] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches*, Experian, (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited July 7, 2023).

188. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud.

189. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the ransomware attack into its systems and, ultimately, the theft of its patients' Private Information.

190. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[75]

191. For example, different PII and PHI elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[76] Based upon information and belief, the unauthorized parties utilized the Private Information they obtained through the Data Breach to obtain additional information from Plaintiffs and Class Members that was misused.

192. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

---

[75] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010).

[76] *See id.* (evaluating privacy framework for entities collecting or using consumer data can be "reasonably linked to a specific consumer, computer, or other device").

193. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if payment card information was not involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiffs.

194. Given these facts, any healthcare or other type of entity that transacts business with patients or customers and then compromises the privacy of its patients' or customers' Private Information has thus deprived them of the full monetary value of the transaction with the entity.

195. Acknowledging the damage to Plaintiffs and Class Members, Defendant instructed patients like Plaintiffs to "review the statements you receive from your health insurer" and call the insurer "immediately" if fraudulent charges appear. Plaintiffs and Class Members now face an impending, substantial risk of identity theft and medical insurance fraud.

196. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

L. The Data Breach's Impact on Plaintiffs & Class Members

197. Onix received Plaintiffs' PII/PHI in connection with providing certain devices to them. In requesting and maintaining Plaintiffs' PII/PHI for business purposes, Onix expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiffs' PII/PHI. Onix, however, did not take proper care of Plaintiffs' PII/PHI, leading to its exposure to and exfiltration by cybercriminals as a direct result of Onix's inadequate data security measures.

198. On or around May 26, 2023, Onix sent Plaintiffs a notice concerning the Data Breach. The letter stated that Onix experienced a cybersecurity attack and that the incident may

have resulted in unauthorized access to Plaintiffs' PII/PHI stored on Onix's systems. The notice stated that the compromised information that was present on the impacted files included one or more of the following data elements: name, date of birth, patient number, social security number, financial account number, and/or health insurance information. Onix also offered identity theft protection services through Equifax, Experian and TransUnion, but only for a period of one year.

199. Onix's conduct, which allowed the Data Breach to occur, caused Plaintiffs significant injuries and harm, including but not limited to, the following—Plaintiffs immediately devoted (and must continue to devote) time, energy, and money to: closely monitoring their medical statements, bills, records, and credit and financial accounts; changing login and password information on any sensitive account even more frequently than they already do; more carefully screening and scrutinizing phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; searching for suitable identity theft protection and credit monitoring services and paying for such services to protect themselves; and placing fraud alerts and/or credit freezes on their credit file. Plaintiffs have taken or will be forced to take these measures in order to mitigate their potential damages as a result of the Breach.

200. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs will need to maintain these heightened measures for years, and possibly their entire lives. Consumer victims of data breaches are more likely to become victims of identity fraud.[77]

201. Plaintiffs greatly value their privacy, especially while receiving medical services and/or devices. Plaintiffs and Class Members did not receive the full benefit of their bargain when paying for medical services, and instead received services that were of a diminished value to those

[77] *See 2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study (last visited July 6, 2023).

described in their agreements with their respective healthcare institutions that had made agreements with Onix for the benefit and protection of Plaintiffs and Class Members and their respective Private Information. Plaintiffs and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

202. Plaintiffs and Class Members would not have obtained medical services and/or devices from Onix, or paid the amount they did to receive such, had they known that Onix would negligently fail to adequately protect their PII/PHI. Indeed, Plaintiffs paid Onix for medical devices with the expectation that Onix would keep their PII/PHI secure and inaccessible from unauthorized parties. Plaintiffs and Class Members would not have obtained services from their medical providers had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

203. Plaintiffs and Class Members have lost confidence in Onix, as a result of the Data Breach.

204. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise commit the identity theft and misuse of Plaintiffs' and Class members' Private Information as detailed above, and Plaintiffs and members of the Class are at a heightened and increased substantial risk of suffering identity theft and fraud.

205. Plaintiffs are also at a continued risk of harm because their PII/PHI remains in Onix systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Onix fails to undertake the necessary and appropriate data security measures to protect the PII and PHI in its possession.

206. As a result of the Data Breach, and in addition to the time Plaintiffs have spent and anticipate spending to mitigate the impact of the Data Breach on their lives, Plaintiffs have also suffered emotional distress from the public release of their PII and PHI, which they believed would be protected from unauthorized access and disclosure. The emotional distress they have experienced includes anxiety and stress resulting from the unauthorized bad actors viewing, selling, and misusing their PII and PHI for the purposes of identity theft and fraud.

207. Additionally, Plaintiffs have suffered damage to and diminution in the value of their highly sensitive and confidential PII/PHI—a form of property that Plaintiffs entrusted to Onix and which was compromised as a result of the Data Breach Onix failed to prevent. Plaintiffs have also suffered a violation of their privacy rights as a result of Onix's unauthorized disclosure of their PHI/PII.

208. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

209. Some of the injuries and risks associated with the loss of Private Information have already manifested themselves in Plaintiffs' and other Class Members' lives. Each Class Member received a cryptically written notice letter from Defendant stating that their Private Information was released, and that they should remain vigilant for fraudulent activity, with no other explanation of where this Private Information could have gone, or who might have access to it.

210. In addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

211. Plaintiffs bring all counts, as set forth below, individually and as a class action, pursuant to the provisions of the Fed. R. Civ. P. 23, on behalf of a Class defined as:

> All persons in the United States who had their Private Information submitted to Defendant or Defendant's affiliates and/or whose Private Information was compromised as a result of the Data Breach, including all persons who were sent notice of the Data Breach.

212. Excluded from the Class are Onix's officers and directors; any entity in which Onix has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Onix. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

213. Plaintiffs reserve the right to amend or modify the Class or Class definitions as this case progresses.

214. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

215. **Numerosity, Fed. R. Civ. P. 23(a)(1)**: The Members of the Class are so numerous that joinder of all of them is impracticable. According to a filing with the U.S. Department of Health and Human Services, the Data Breach impacted 319,500 people.[78]

[78] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited July 6, 2023)

216. **Commonality, Fed. R. Civ. P. 23(a)(2):** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Onix unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether Onix failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Onix's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, HIPAA;

d. Whether Onix's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Onix owed a duty to Class Members to safeguard their Private Information;

f. Whether Onix breached the duty to Class Members to safeguard their Private Information;

g. Whether Onix knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Onix should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Onix's misconduct;

j. Whether Onix's conduct was negligent;

k. Whether Onix breached implied contracts with Plaintiffs and Class Members;

l. Whether Onix was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

m. Whether Onix failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

217. **Typicality, Fed. R. Civ. P. 23(a)(3)**: Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach. Further, there are no defenses available to Defendant that are unique to Plaintiffs.

218. **Adequacy of Representation, Fed. R. Civ. P. 23(a)(4):** Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and experienced in litigating class actions.

219. **Injunctive Relief, Fed. R. Civ. P. 23(b)(2):** Defendant has acted and/or refused to act on grounds that apply generally to the Class therefore making injunctive and/or declarative relief appropriate with respect to the Class under 23(b)(2).

220. **Superiority, Fed. R. Civ. P. 23(b)(3):** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Onix. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

221. Onix has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

222. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Onix failed to timely and adequately notify the public of the Data Breach;

b. Whether Onix owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Onix's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Onix's failure to institute adequate protective security measures amounted to negligence;

e. Whether Onix failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

223. Finally, all members of the proposed Class are readily ascertainable. Onix has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Onix.

CAUSES OF ACTION

FIRST COUNT

Negligence
(*On Behalf of Plaintiffs and the Class*)

224. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

225. Onix required customers, including Plaintiffs and Class Members, to submit non-public Private Information in the ordinary course of healthcare services.

226. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, Onix owed a duty of care to use reasonable means to secure and safeguard its computer system—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Onix's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

227. Onix owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

228. Plaintiffs and the Class are a well-defined, foreseeable, and probable group of patients that Onix was aware, or should have been aware, could be injured by inadequate data security measures.

229. Onix owed numerous duties to Plaintiffs and the Class, including the following:

- To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;
- To protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
- To implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

230. A large depository of highly valuable health care information is a foreseeable target for cybercriminals looking to steal and profit from that sensitive information. Onix knew or should have known that, given its repository of a host of Private Information for hundreds of thousands of patients posed a significant risk of being targeted for a data breach. Thus, Onix had a duty to reasonably safeguard its patients' data by implementing reasonable data security measures to

protect against data breaches. The foreseeable harm to Plaintiffs and the Class of inadequate data security created a duty to act reasonably and safeguard the Private Information.

231. Onix's duty of care to use reasonable security measures also arose as a result of the special relationship that existed between Onix and patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Onix was in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

232. Onix's duty to use reasonable security measures under HIPAA required Onix to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

233. In addition, Onix has a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

234. Onix's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Onix is bound by industry standards to protect confidential Private Information.

235. Onix breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Onix includes, but is not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

236. It was foreseeable that Onix's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

237. Onix's conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect the Private Information and failing to provide Plaintiffs and Class Members with timely notice that their sensitive Private Information had been compromised.

238. Neither Plaintiffs nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

239. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members suffered damages as alleged above.

240. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

241. Plaintiffs and Class Members are also entitled to injunctive relief requiring Onix to, *e.g.,* (i) strengthen their data security systems and monitoring procedures; (ii) submit to future

annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT

Negligence *Per Se*
(*On Behalf of Plaintiffs and the Class*)

242. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

243. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Onix has a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

244. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et seq.*, Onix had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

245. Pursuant to HIPAA, Onix had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* definition of encryption at 45 C.F.R. § 164.304.

246. Onix breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

247. Onix's failure to comply with applicable laws and regulations constitutes negligence *per se*.

248. But for Onix's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

249. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Onix's breach of its duties. Onix knew or should have known that it was failing to meet its duties, and that Onix's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

250. As a direct and proximate result of Onix's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

THIRD COUNT

Breach of Implied Contract
(*On Behalf of Plaintiffs and the Class*)

251. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

252. Plaintiffs and the Class Members entered into implied contracts with Onix under which Onix agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members that their information had been breached and compromised.

253. Plaintiffs and the Class were required to and delivered their Private Information to Onix as part of the process of obtaining services provided by Onix. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Onix in exchange for services.

254. Onix solicited, offered, and invited Class Members to provide their Private Information as part of Onix's regular business practices. Plaintiffs and Class Members accepted Onix's offers and provided their Private Information to Onix.

255. Onix accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services for Plaintiffs and Class Members.

256. In accepting such information and payment for services, Plaintiffs and the other Class Members entered into an implied contract with Onix whereby Onix became obligated to reasonably safeguard Plaintiffs' and the other Class Members' Private Information.

257. In delivering their Private Information to Onix and paying for healthcare services, Plaintiffs and Class Members intended and understood that Onix would adequately safeguard the data as part of that service.

258. Upon information and belief, in its written policies, Onix expressly and impliedly promised to Plaintiffs and Class Members that they would only disclose protected information and other Private Information under certain circumstances, none of which related to a Data Breach as occurred in this matter.

259. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state or federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

260. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

261. Plaintiffs and the Class Members would not have entrusted their Private Information to Onix in the absence of such an implied contract.

262. Had Onix disclosed to Plaintiffs and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and the other Class Members would not have provided their Sensitive Information to Onix.

263. Onix recognized that Plaintiffs' and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

264. Plaintiffs and the other Class Members fully performed their obligations under the implied contracts with Onix.

265. Onix breached the implied contract with Plaintiffs and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

266. As a direct and proximate result of Onix's conduct, Plaintiffs and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

FOURTH COUNT

Unjust Enrichment
(*On Behalf of Plaintiffs and the Class*)

267. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

268. This count is pleaded in the alternative to Count 3 (breach of implied contract).

269. Upon information and belief, Onix funds its data security measures from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

270. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Onix.

271. Plaintiffs and Class Members conferred a monetary benefit on Onix. Specifically, they purchased medical services from Onix and/or its agents and in so doing provided Onix with their Private Information. In exchange, Plaintiffs and Class Members should have received from Onix the services that were the subject of the transaction and have their Private Information protected with adequate data security.

272. Onix knew that Plaintiffs and Class Members conferred a benefit which Onix accepted. Onix profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

273. Plaintiffs and Class Members conferred a monetary benefit on Onix, by paying Onix as part of rendering medical services, a portion of which was to have been used for data security measures to secure Plaintiffs' and Class Members' Personal Information, and by providing Onix with their valuable Personal Information.

274. Onix was enriched by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Onix instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Onix's failure to provide the requisite security.

275. Under the principles of equity and good conscience, Onix should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Onix failed to implement appropriate data management and security measures that are mandated by industry standards.

276. Onix acquired the monetary benefit and Personal Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

277. If Plaintiffs and Class Members knew that Onix had not secured their Personal Information, they would not have agreed to provide their Personal Information to Onix.

278. Plaintiffs and Class Members have no adequate remedy at law.

279. As a direct and proximate result of Onix's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their Personal Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Onix's possession and is subject to further unauthorized disclosures so long as Onix fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

280. As a direct and proximate result of Onix's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

281. Onix should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Onix should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Onix's services.

FIFTH COUNT

Breach of Fiduciary Duty
(*On Behalf of Plaintiffs and the Class*)

282. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

283. In light of the special relationship between Onix and Plaintiffs and Class Members, Onix became a fiduciary by undertaking a guardianship of the Private Information to act primarily for Plaintiffs and Class Members (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Onix do store.

284. Onix had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with its patients, in particular, to keep secure their Private Information.

285. Onix breached its fiduciary duty to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

286. Onix breached its fiduciary duty to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

287. Onix breached its fiduciary duty owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

288. Onix breached its fiduciary duty to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

289. As a direct and proximate result of Onix's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual

identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Onix's possession and is subject to further unauthorized disclosures so long as Onix fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Onix's services they received.

290. As a direct and proximate result of Onix's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a. For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representative and their counsel as Class Counsel;

b. For equitable relief enjoining Onix from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c. For equitable relief compelling Onix to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Onix's wrongful conduct;

e. Ordering Onix to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded and

j. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiffs hereby demand a trial by jury on all claims so triable in this action.

Dated: July 7, 2023

Respectfully submitted,

By: */s/ Paul Costa, Esq.*

FINE, KAPLAN AND BLACK R.P.C.
One South Broad Street, 23rd Floor
Philadelphia, PA 19107
Tel: (215) 567-6565
Fax: (215) 568-5872
pcosta@finekaplan.com

ALMEIDA LAW GROUP LLC
David S. Almeida*
Elena A. Belov*
849 W. Webster Avenue
Chicago, Illinois 60614
Tel: (312) 576-3024
david@almeidalawgroup.com
elena@almeidalawgroup.com

**Pro Hac Vice Application Forthcoming*

Attorneys for Plaintiffs & the Class